Warring Germs

The increasing threat of bioterrorism calls for a new security framework

By **Reynolds M. Salerno, Ph.D.** and **Lauren T. Hickok**

The tragic events of September 2001 and the subsequent dissemination of Bacillus anthracis through the United States postal system underscored the dangers to national and international security posed by terrorist attacks, especially those involving pathogenic microorganisms and toxins.

As we now know, bioterrorism can have high national and international consequences. Natural incidents of highly infectious disease, such as the recent SARS outbreak, which infected over 8,000 people and killed almost 800, demonstrate both the potential devastation of a bioterrorist event as well as the international characteristics of rapidly spreading disease.

Like other nations, India has recently suffered a number of serious infectious disease outbreaks. In 1996, an occurrence of Dengue Hemorrhagic Fever struck Delhi, resulting in nearly 9,000 infected individuals and over 300 deaths. In 1999, 965 people were infected and 200 people died from an outbreak of Japanese Encephalitis in Andhra Pradesh.

And in the agricultural sector, India experiences an outbreak of endemic Foot and Mouth Disease (FMD) – the most infectious animal disease – approximately once every decade. The consequences of a non-endemic FMD outbreak, to which the animal population may have no resistance, could be devastating. For instance, an outbreak of FMD in the United Kingdom in 2001 caused economic losses of approximately $8 billion.

What is particularly worrisome is that the consequences of a bioterrorist attack, employing an exotic and highly infectious human or animal agent, could far exceed those caused by a natural outbreak of an endemic disease. Moreover, today's wide availability of these exotic organisms, as well as advanced biotechnology and microbiological expertise, makes biological weapons more accessible to terrorists than ever before.

Internationally, many different strategies are now being applied to combat the proliferation and use of biological weapons. Most strategies – such as increasing the effectiveness and availability of vaccines and therapies, improving disease surveillance and detection, building public health capacities, and developing biosensor technologies – are reactionary in nature. They focus on improving the ability to detect and respond to a bioterrorist event after it has occurred. The international community has also begun employing preventive strategies. One of the principal strategies in this category is biosecurity, which is the protection of dangerous pathogens and toxins.

The Concept of Biosecurity

Biosecurity aims to stop proliferation before it starts by protecting dangerous pathogens and toxins – the basic building blocks of a biological weapon – against theft from and sabotage at bioscience institutions. By preventing potential bioterror-

ists or proliferant states from acquiring certain dangerous biological materials, biosecurity provides the first line of defence against both state-based biological weapons proliferation and bioterrorism.

Thousands of bioscience facilities around the world conduct critical and beneficent human, animal, and plant health research on pathogens and toxins that could be used as biological weapons. Ironically, the rapid growth of the global biomedical and bioscience industry has resulted in a corresponding increase in the number of facilities that store, use, and transport dangerous pathogens and toxins.

Like many other nations, India is experiencing a significant expansion of biotechnology research and commerce. This Indian industry is expected to grow at a rate of 15 per cent per year, reaching a value of more than $9 billion by 2005. This rapid development has been spurred by substantial government support. In 2001, the Department of Biotechnology promulgated a national vision for the industry that included the construction of many biotech parks, including the Tamil Nadu Industrial Centre for Life Sciences Bio-Park and Kerala Biotech Park. These projects represent additions to an already considerable infrastructure that includes Genome Valley and Pune Biotech Park, among others.

Despite concerns about bioterrorism and the propagation of facilities that house dangerous pathogens and toxins, biosecurity – the concept of protecting those materials from theft and sabotage – has not been widely embraced internationally.

Part of the reason is that government, academic, and private biological research communities have not been accustomed to operating in security-conscious environments. Until recently, governments had not required security at biological research facilities. Many biological scientists perceived traditional security applied to microbiology laboratories as ineffective, intrusive, expensive, and likely to obstruct or jeopardise vital biomedical and bioscience research.

Another reason for the general lack of biosecurity is that the concept itself is relatively new. In the United States, biosecurity regulations have been in place for less than one year. And although the international community has begun discussing biosecurity at meetings of States Parties to the Biological Weapons Convention, the international microbiological community has not yet reached a consensus on a clear definition of biosecurity. No international biosecurity standards currently exist.

But protecting dangerous pathogens and toxins from theft and sabotage should not be postponed until an international organisation promulgates biosecurity guidelines. Today's significant biological weapons and bioterrorist threat justifies improving control and oversight over certain biological material that could be used as a weapon. Individual nations can and should take responsibility for securing their own collections of high consequence biological agents and toxins. Such steps will reduce the likelihood of bioterrorism and stem the proliferation of biological weapons.

Biosecurity Methodology

Although it is essential and appropriate to establish biosecurity systems, practices, and procedures that deter and detect the malicious diversion of these biological materials, it is critically important to strike an appropriate balance between protection of biological material that could be used in a biological weapon and preservation of an environment that promotes legitimate and lifesaving microbiological research. Designing a biosecurity system that does not jeopardise research at biomedical and bioscience facilities requires a familiarity with bioscience and the materials that require protection.

It is important to recognise that, although certain biological agents have the potential to cause serious harm to the health and economy of a population if misused, all have legitimate medical, commercial, and defensive applications. The possession of any one of these inherent 'dual use' materials does not necessarily signal an intention to use that material as a weapon.

In designing a security system, one must be cognizant of several challenges to protecting microorganisms and toxins. Biological agents are widespread. They exist in nature and are globally distributed in research laboratories, collection centres, and clinical facilities. In addition, biological agents are living, self-reproducing organisms, the volumes of which continually change throughout legitimate research activities. They can be found in microscopic amounts in a number of locations within a facility, including freezers, incubators, infected animals and their waste. Finally, because microorganisms do not emit detectable or recognisable amounts of energy, they cannot be identified with current standoff detection systems.

An effective biosecurity system should address all of these unique challenges in order to achieve a balance between security and research priorities. To attain these goals, the system designers should employ a risk management approach that recognises that no security system can protect every asset against every conceivable threat. Therefore, the biosecurity methodology should establish clear objectives for the biosecurity system by defining which assets should be protected against which threats. The system designers and institutional managers should identify and prioritise the facility's assets, identify the adversaries who would attempt to divert or steal those assets, develop scenarios of undesirable events involving those assets and threats, and conduct a security risk assessment of the scenarios based on their probability and consequences.

It is often appropriate for institutional managers to decide not to protect against adversaries who would conduct an overt external assault to steal agents. First, these agents are not unique materials; they can be isolated in nature and exist in laboratories throughout the world. Second, an overt attack using force would signal authorities to respond with medical and/or agricultural countermeasures that could mitigate the consequences of a bioterrorist attack.

Bioscience facilities should concern themselves with defending against an insider who has approved access. An insider who is willing to divert a primary asset may be a disgruntled employee, or one who is financially desperate, personally threatened, psychologically unstable, or motivated by any number of other reasons. Insiders are familiar with the protocols of the institution, and have knowledge of, and

What is particularly worrisome is that the consequences of a bioterrorist attack, employing an exotic and highly infectious human or animal agent, could far exceed those caused by a natural outbreak of an endemic disease

India's biotechnology research and commerce industry is expected to grow at a rate of 15 per cent per year, reaching a value of more than $9 billion by 2005

access to, the critical assets.

Bioscience facilities should also concern themselves with outsiders who would attempt to steal a biological agent covertly. This type of adversary would likely avoid detection and abort the diversion attempt if he thought he would be caught. These covert outsiders could include visiting scientists, students, and short-term maintenance workers.

Components of a Biosecurity System

An effective biosecurity system includes many different components and should not rely on physical security and technologies alone. In fact, the most important aspects of a biosecurity system are procedural and cultural – elements that do not require large expenditures of resources. For example, a biosecurity system should physically consolidate, to the extent possible, all dangerous pathogens and toxins. Access to those biological materials should then be controlled by a combination of door locks or access controls and limiting the number of authorised personnel.

The personnel who receive permission to access these areas should provide evidence that they have a legitimate need to handle, use, or transport dangerous pathogens or toxins, and that they have completed specific biosafety and biosecurity training. In addition, these personnel should be subject to a level of background screening that demonstrates their honesty and reliability. Procedures should also be established for escorting visitors and support personnel who only need occasional access to areas where dangerous pathogens and toxins are located.

A biosecurity system should establish control and accountability of dangerous pathogens and toxins by documenting exactly what materials exist at the facility, where in the facility they are located, who has access to them, and who is responsible for them. Material control and accountability procedures should avoid trying to apply quantitative material-balance inventory accounting principles, which are impossible to achieve in a biological environment.

Because dangerous pathogens and toxins are often transferred between facilities and shared among researchers, it is important for a biosecurity system to implement procedures to document, account for, and control both internal and external transfers of that material. Ideally, the procedures would demonstrate continuous custody of dangerous pathogens and toxins during both internal and external transfers.

All of the components of the biosecurity system should be documented in a biosecurity plan, which should be regularly reviewed and revised. In addition, an incident response plan should be written as well as regularly reviewed and revised. These core texts of the biosecurity system, as well as the many biosecurity policies and procedures, indicate that there is also a genuine need for information control and oversight. Biosecurity systems should include procedures for handling, using, and storing certain sensitive information related to the dangerous pathogens and toxins and the various methods for accessing and protecting them.

Perhaps most importantly, a biosecurity system should include a security programme management infrastructure that develops and maintains the biosecurity plan and incident response plan, and conducts regular security training for the institution's staff. Creating and sustaining a biosecurity culture is the responsibility of the security programme management staff.

Achieving Biosecurity

The increased biological weapons and bioterrorist threat justifies improving control and oversight over those biological materials that could be used to cause a devastating or highly disruptive event. Individual nations can and should take responsibility for securing their own collections of high consequence pathogens and toxins. First on the agenda should be the promulgation of legislation that requires facilities that possess dangerous biological agents to establish and maintain biosecurity systems. A government should also establish national biosecurity guidelines and standards, and policies and procedures for implementing biosecurity at specific facilities. Such measures would limit accessibility to dangerous biological materials, thus reducing the likelihood of bioterrorism and stemming the proliferation of biological weapons. •

Reynolds M. Salerno, Ph.D., is a Principal Member of the Technical Staff at Sandia National Laboratories in Albuquerque, NM, USA. He is the director of Sandia's biosecurity programme. Lauren T. Hickok is a biosecurity analyst at Sandia. Sandia is a multiprogramme laboratory operated by Sandia Corporation, a Lockheed Martin Company for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.